PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-050665
(43)Date of publication of application : 21.02.1995

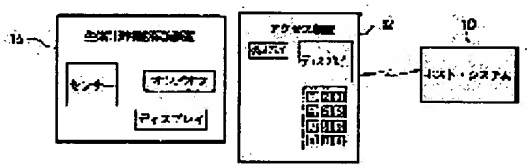
(51)Int.CI. H04L 9/32
G06T 7/00

(21)Application number : 05-196393
(22)Date of filing : 06.08.1993

(71)Applicant : KUMAHIRA SAFE CO INC
(72)Inventor : ROORENSU ESU GARUMAN
ERITSUKU EDOWAAZU
NOOMAN FUASUTO

(54) IDENTITY CONFIRMING DEVICE AND ITS METHOD

(57)Abstract:
PURPOSE: To provide an identity confirming device equipped with an improved secrecy protecting mechanism with convenience and the exactness of secrecy protection, in which it is possible to facilitate a countermeasure to a load that a person using an electronic type communication system stores plural numbers and pass words, and abuse due to the loss and robbery of a card.
CONSTITUTION: An organism measuring secrecy protecting device 14 receives the input of organism measurement information (voice, signature, and fingerprint or the like) from a user, decides a correlation factor by comparing it with a model, and prepares a token by integrating the correlation factor with a fixed code, time fluctuation code, or challenge code. This is inputted to an access device 12 connected with a host system 10, and transmitted to the host system 10, and whether or not an access is permitted is decided by processing the token. Also, the organism measuring secrecy protecting device 14 (for example, an IC card) is constituted of a sensor which detects information, processor which prepares the token, and display.



LEGAL STATUS

[Date of request for examination] 06.08.1993
[Date of sending the examiner's decision of rejection] 16.04.1996
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－50665

(43)公開日　平成７年(1995)２月21日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/32					
Ｇ０６Ｔ　7/00					
			Ｈ０４Ｌ　9/00	Ａ	
			Ｇ０６Ｆ　15/62	４６５　Ａ	

審査請求　有　　請求項の数10　ＯＬ　（全７頁）

(21)出願番号　特願平5－196393

(22)出願日　平成５年(1993)８月６日

(71)出願人　000142540
株式会社熊平製作所
広島県広島市南区宇品東２丁目４番34号

(72)発明者　ローレンス　エス　ガルマン
アメリカ合衆国、カリフォルニア州
94020ラホンダ、ボックス30、ルート30

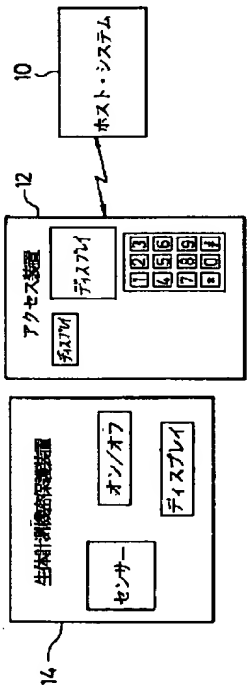
(72)発明者　エリック　エドワーズ
アメリカ合衆国、カリフォルニア州
94025メンロ　パーク、ナンバー３、パイン　ストリート　1143

(74)代理人　弁理士　磯野　道造

最終頁に続く

(54)【発明の名称】　本人確認装置及びその方法

(57)【要約】
【目的】電子式通信システムを利用する人が多数の番号とパスワードを記憶する負担並びにカードの紛失盗難による悪用に対処するため、使用が便利で機密保護の確実な改善された機密保護メカニズムを備えた本人確認装置を提供する。
【構成】生体計測機密保護装置１４がユーザーからの生体計測情報（声、署名、指紋、等）のインプットを受信し、雛形と比較して相関ファクタを決定し、その相関ファクタと固定コード及び時間変動コード或いはチャレンジ・コードとを組み合わせてトークンを生成し、それをホスト・システム１０に連結されたアクセス装置１２に入れてホスト・システム１０へ送信し、トークンを処理してアクセスを許可するかどうか決定する。生体計測機密保護装置１４（例えばＩＣカード）は情報を検知するセンサー１８、トークンを生成するプロセッサ２２及びデイスプレイ２０より成る。



1

【特許請求の範囲】

【請求項１】遠隔ホスト・システムのユーザーの身元を許可されているユーザーのものと照合確認するために使用する本人確認装置で下記よりなる：

（１）ユーザーから生体計測情報を受信する手段；

（２）既得の許可されているユーザーの生体計測情報と固定コードと共に容認限界レベル・データを貯蔵するメモリ手段；

（３）ユーザーからの当該生体計測情報を当該既得生体計測情報と比較し且つ相関ファクタを作成する比較手段；

（４）当該相関ファクタを当該容認限界レベル・データと比較し，認証コードを含む送信可能コードを作成する信号生成手段；

（５）当該信号生成手段より当該送信可能コードを受信し、当該認証コードを含む当該送信可能コードをホスト・システムへ送信してホスト・システムへのアクセスをユーザーに許諾するのかどうかホスト・システムで決定する送信手段。

【請求項２】当該信号生成手段は更に当該認証コードと当該固定コードを組み合わせて当該送信手段へ送信するための送信可能コードを作成しホスト・システムへのアクセスをユーザーに許諾するのかどうかをホスト・システムで決定するためホスト・システムへ引き続き送信することを特徴とする請求項１に記載の本人確認装置。

【請求項３】時間変動コードを当該メモリ手段へインプットする手段を含みまた当該信号手段は当該第一認証コードを当該時間変動コードと組み合わせて、当該送信手段へ送信すべき送信可能コードを作成し、ホスト・システムへのアクセスをユーザーに許諾するのかどうかホスト・システムが決定するためホスト・システムへ更に送信することを特徴とする請求項２に記載の本人確認装置。

【請求項４】チャレンジ・コードを当該信号生成手段にインプットする手段を含み、また当該信号生成手段は当該認証コードと当該チャレンジ・コードを組合わせて送信可能コードを作成し、また当該送信手段はホスト・システムへのアクセスをユーザーに許諾するかどうかをホスト・システムが決定するためホスト・システムへ当該送信可能コードを送信することを特徴とする請求項２に記載の本人確認装置。

【請求項５】当該送信可能コードは数字であることを特徴とする請求項４に記載の本人確認装置。

【請求項６】ホスト・システムのユーザーの身元を許可されたユーザーのものとの照合確認用に使用する本人確認装置で下記よりなる：

（１）生体計測インプットをユーザーから受信し、またそれに対する回答のインプット信号を作成するインプット手段；

（２）許可されているユーザーの生体計測情報を貯蔵し、また許容レベルデータを貯蔵するメモリ手段；

（３）下記よりなる当該インプット手段と当該メモリ手段とに連絡するデータ処理手段：

（ｉ）当該インプット手段から当該インプット信号を受信する；

（ｉｉ）当該メモリ手段から許可されているユーザーの生体計測情報を受信する；

（ｉｉｉ）当該インプット信号と許可されているユーザーの当該生体計測情報を比較する；

（ｉｖ）類似信号を作成する。

（４）当該限界容認レベル・データを当該類似信号と比較し認証コードを含む送信可能コードを作成する信号生成手段；

（５）当該信号生成手段から当該送信可能コードを受信し、また当該認証コードを含む当該送信可能コードをホスト・システムへ送信して、当該ホスト・システムへのアクセスをユーザーに許諾するのかどうかを当該ホスト・システムが決定する送信手段。

【請求項７】時間コード信号を生成し、当該時間コード信号を当該メモリ手段へインプットする手段を含み、また当該信号生成手段は当該時間コード信号と当該認証コードを組み合わせて当該送信手段へ送信する送信可能コードを生成することを特徴とする請求項６に記載の本人確認装置。

【請求項８】ユーザーの身元が許可されているユーザーのものであることを認証し、ホスト・システムへのアクセスを安全保障する方法で下記ステップより成る：

（１）ユーザーの生体計測インプットを受信し；

（２）その生体計測インプットを貯蔵されている雛形と比較して相関ファクタを生成し；

（３）当該相関ファクタを前もって決定した許容限界レベル・データと比較し送信可能コードを生成し；

（４）当該送信可能コードを当該ホスト・システムへ送信し；

（５）受信した送信可能コードからホスト・システムへのアクセスを許諾するかどうかをホスト・システムで決定する。

【請求項９】当該相関ファクタを当該容認限界レベル・データと組み合わせて、認証コードを生成し、それを更に時間変動コードと組み合わせて送信可能コードを生成してアクセスを許諾するかどうか決定するために使用するホスト・システムへ送信することを特徴とする請求項８に記載の方法。

【請求項１０】そのように生成した当該送信可能コードは更にチャレンジ・コードと組み合わせて、当該ホスト・システムへ送信するため数字コードを作成し、ホスト・システムにおいてアクセスを許可するかどうかを決定することを特徴とする請求項９に記載の方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明はコンピュータ及びその他、類似の装置の電子式ホスト・システム（上位システム）へのアクセスを保護するための識別並びに機密保護システムを備えた本人確認装置に関する。更に具体的には，この発明は機密保護用トークン（送信許可証）を誘導するためのシード（種）として使用する生体計測を行い、前記ホスト・システムへのアクセスを許可すべきかどうかを決定するため、そのトークンを前記ホスト・システムへ伝達する本人確認装置に関するものである。

【０００２】

【従来の技術】電子式通信システムを使用する人は誰でもアクセス出来る可能性のある個人情報の増大に伴い、かかる情報へのアクセスを保護するための機密保護の方策を提供する必要も増大している。銀行取引き用の自動テラー・マシン（出納機械）により特定の銀行カードを所有し、またそれに対応する個人の識別番号（ＰＩＮ）を記憶している人は、その銀行口座へアクセスしてお金の引き出し或いは振替えが可能である。また、コンピュータにより請求書或いは商店への支払も可能である。電子式の取引きを行う機会の増大に伴い、電子式の盗難の危険も増大する。かくして、より効果的な機密保護のメカニズムが必要である。

【０００３】通常の機密保護メカニズムは個人識別番号（ＰＩＮ）と機密保護トークンを使用する。個人識別番号は個人を識別し、ホスト・システム（例えば、銀行取引きシステム）へのアクセスを許可するために使用する。機密保護トークンは個人のキー例えば特定の固定数値、及び公開キー例えば時間変動数値、から誘導した予想出来ないコードである。例えば、あるパスワード（固定キー）を時間変動情報に基づきコード化する。それからそのトークンは前記ホスト・システムに送られてトークンを解読しパスワードに戻す。前記トークンはこのようにして特定の固定数値が送信中に識別されないように機密保護を行う。例え、送信中に悪人がトークンを受信して、その受信したトークンを再び使用してもホスト・システムへアクセス出来ない。何故なら時間で変動する“公開キー”は変わっているからである。

【０００４】このように、個人識別番号はユーザーの識別を行うのに対し、トークンは送信の機密保護を行う。秘密コードとトークンと共に生体計測情報の使用に関する公知文献は米国特許第４、９９８、２７９号名称『予知出来ないコードと個人の生体特性を利用して個人の確認を行う方法と装置』（Ｗｅｉｓｓ特許）であり、参考のため、その全開示事項をここに取り上げる。その開示事項によると、クレジット・カードの大きさのコンピュータで或る秘密の“固定”コード（即ちＰＩＮ）と公開の“時間で変わる”コード（即ち日時）からトークンを作る。そのトークンはカードに表示されるので、ユーザーはそのトークンをアクセス・マシンに入れることが出来る。

【０００５】前記トークンは生体特性情報と組み合わせて入れる。例えば、トークンはユーザーに圧力感知板上にトークン番号を書かせるか、電話でトークン番号を読み上げさせて入れることが出来る。当該アクセス確認システムは前記トークンを比較して有効性を確認しその生体インプット（例えば、声、又は署名）と比較し、許可されているユーザーからのものかどうかを確認する。このように生体特性情報は許可されているユーザーの識別のため、使用する。

【０００６】個人識別番号と機密保護トークンを使用する別の普通の機密保護メカニズムはチャレンジ／リスポンス・トークンであり、内部で生成される時間変動数値からでなく、ホスト・システムが出すチャレンジ番号から動的機密保護パスワードを作成する。その一つの実例に、カリフォルニア州コンコルド市のエニグマ・ロジック社製造のセイフワード・アクセス・カードがある。

【０００７】

【発明が解決しようとする課題】個人識別番号とトークンの問題点は正当なユーザーが前記の番号或いはパスワードを記憶していなければならない事である。沢山の番号或いはパスワードを持っているユーザーにとっては、記憶するのは負担となることがある。更に、長距離電話カードのようなカードには直接個人のアクセス・コードまで印刷されているものがあるので、もしカードを紛失或いは盗難にあった場合、それを見付けた人は正当なユーザーの費用で前記システムにアクセス出来る。従って、使用が便利で且つ機密保護を保証する改善された機密保護メカニズムが必要である。

【０００８】

【課題を解決するための手段】上記課題を解決するため、この発明では生体計測情報を、それに対応した機密保護トークンを生成するため生体計測機密保護装置へ入力する。前記生体計測情報はトークンを発生させるための“シード”の一部として使用する。そのトークンはホスト・システム又はアクセス・システムへ伝達されて当該ホスト・システムへのアクセスを許可して良いかどうか決定する。

【０００９】その一つの特長は、前記生体計測機密保護メカニズムがユーザーの生体計測情報（即ち、サイン、指紋、声紋）の雛形を貯蔵することである。前記ホスト・システムにアクセスするためユーザーは相当する生体計測情報を前記機密保護メカニズムに入れる。前記メカニズムはその入力を雛形と照合し、その照合に基づきトークンを生成させて表示する。当該ユーザーが前記トークンをホスト・システムに伝達すると、そのトークンを解読しアクセスを許可できるかどうかを決定する。更に具体的には、前記トークンは、生体計測の比較、並びに時間変動数値の結果から誘導する。

【００１０】この発明の他の方法は、前記トークンを時間変動数値からではなく、上記生体計測の比較と、前記

ホスト・システムからのユーザー入力チャレンジ・コードの結果から誘導する。更に別の方法として、ユーザーがキー盤、記入、又は声のいずれかで前記チャレンジ・コードを当該装置にインプットして、前記生体計測情報を集める。

【００１１】具体的には、当該生体計測機密保護メカニズムはプロセス（処理）装置、メモリ及び生体計測センサーを有するＩＣカードである。当該メモリは照合計算方式と共に、許可されているユーザーの生体計測情報の雛形を貯蔵している。当該カードの所有者の生体計測情報を入れると、そのプロセッサが当該計算方式を実行する。当該照合計算方式は雛形のデータ、生体計測インプット、固定コード（即ち、個人識別番号、刻印連番、口座番号）と時間で変動する自動生成情報を使用してトークンのアウトプットを誘導する。当該トークン・アウトプットはカード所有者が見ることのできるカード上に表示されそして当該ホスト・システムに連結されたアクセス装置に当該トークンを手で入れる。

【００１２】別の方法は、トークンを直接データ通信ラインを通じて当該ホスト・システムへ直接発信し、ユーザーが手で入れる必要をなくしている。ホスト・システムは機密保護アクセスを必要とするか又はそれが付いている電子式システムであればどんなものでもよい。例えば、ホスト・システムは自動テラー・マシン、銀行のコンピュータ・システム或いは機密保護地域にアクセスするための電子式ゲートでもよい。

【００１３】

【実施例】この発明をより良く理解するため添付図面で、下記の通り詳細に説明する。

概略

ホスト・システム１０へのアクセスの機密保護の確保はアクセス装置１２と生体計測機密保護装置１４で行う。通常、ホスト・システム１０はコンピュータ・システムであり、オンラインのバンク・システム又は機密保護地域である。当該ホスト・システム１０（又はホスト地域）は不許可のアクセスに対し機密保護すべき秘密或いは重要な情報を含むものと思考される。かかる情報へのアクセスを保護するためアクセスはアクセス装置１２により制限する。このアクセス装置１２は当該ホスト・システムと通信して許可された人を確認し情報を伝達する。

【００１４】当該アクセス装置はホスト・コンピュータと通信するターミナル及び、ホスト・データベース管理システムを有する銀行ネットワークと通信する自動テラー・マシン及び、コンピュータ・システムに接続された電話、或いは機密保護地域へのアクセスを禁止する電子式ロックでもよい。当該生体計測機密保護装置１４は当該アクセス・プロセスに更に機密保護の能力を追加したものである。

【００１５】この発明では、生体計測機密保護装置１４はユーザーがアクセス装置１２にインプットする機密保護トークンを作成する。その機密保護トークンは生体計測情報、固定コードから作成し、又或る実施例では時間で変わるコード、その次の実施例ではホスト・システムが作成するチャレンジ・コードから作成する。当該生体計測情報は指紋、声紋、或いは筆跡サンプルでもよい。当該機密保護装置１４は生体計測インプットを受けると、その生体計測インプットを貯蔵されている雛形と比較し相関ファクターを誘導する。もしその相関ファクターが設定規定レベル以下であれば、その相関は不成立である。

【００１６】この機密保護装置は当該生体計測の記入が無効であることを表示することができるが、場合によっては当該機密保護装置はその生体計測の記入が無効であったことをユーザーに通知する必要は無い。無効のトークンを表示する代わりにアクセス装置１２にインプットすると、当該ホスト・システム１０へのアクセスは拒否され当該ホスト・システムはアクセスがあったことを知らされる。チャレンジ・コードを使用したこの発明の実施例では、機密保護装置に生体計測インプットを入れることに加え、そのユーザーはチャレンジ・コードを手書き、声又はキー盤へタイプすること等によってインプットし、それらは通常ホスト・システムで作成され、そのユーザーに表示される。

【００１７】チャレンジ・コードを使用する別の代表的な実施例では、ユーザーがそのチャレンジ・コードをインプットする操作をして当該生体計測情報を得る。例えば、ユーザーが声、手書き、又はキー盤へのタイプでチャレンジ・コードをインプットすると、当該機密保護装置は、当該インプットの生体計測測定を行い必要な生体計測情報を生成する。この情報は貯蔵されている雛形と比較され、前述のように、相関ファクタを誘導する。

【００１８】生体計測の記入をうまく行うため、或いはユーザーが生体計測の記入がされなかったことを知らされていない場合は、その相関ファクタを固定コード（即ち、個人識別番号、刻印された連番、口座番号）と組み合わせる。また、或る実施例では、時間で変わるコード（即ち、日時）と組み合わせて機密保護トークンを作成する。チャレンジ・コードの実施例では、相関ファクタを固定コード及びチャレンジ・コードと組み合わせて機密保護トークンを作成する。当該トークンは機密保護装置１４の表示パネルに表示される。ユーザーはそれからアクセス装置１２にそのトークンを記入する。アクセス装置１２はホスト・システム１０にトークンを送り、当該トークンを解読して印加されている固定コードと相関ファクタを識別する。

【００１９】別の実施例では、機密保護装置１４は、ホスト・システムに直接接続され、トークン出力は直接ホスト・システムに送信され、トークンを表示したりユーザーが手で記入する必要はない。その接続は、例えば、

標準データ通信ケーブル或いはその他公知のデータ送信技術を使用して行うことができる。当該トークンを適切に解読するため、生体計測機密保護装置１４はホスト・システム１０に同調されているので、時間変動コードは機密保護メカニズム１４とホスト・システム１０の両方で同じである。

【００２０】チャレンジ・コードの実施例では、ホスト・システムは、チャレンジ・コードを作成し、当該チャレンジ・コードをメモリに保持してトークンを解読する。ホスト・システム１０は固定コードでユーザーを識別し、相関ファクタに基づく識別を照合確認する。ホスト・システム１０は或るユーザー（固定コードで識別された）に割り振られた許可レベルに基づき全部又は一部の記入を許可する。例えば、或るユーザーは指定口座からだけ、電子式で資金の移動を行う事が許される。

【００２１】生体計測機密保護装置

図２は生体計測機密保護装置１４の電子ブロック線図を示す。装置１４は電源１５、オン／オフ・スイッチ１６、生体計測センサー１８、デイスプレイ２０、オンーチップ・ランダム・アクセス・メモリ付きプロセッサ２２、生体計測センサーから生体計測情報を受けるための生体計測インプット部３３、読出し専用メモリ（ＲＯＭ）２４（ＰＲＯＭ，ＥＰＲＯＭ又はその類似品でも可）、時間変動コード・ジェネレータ２６、デイスプレイ駆動装置３０を有する。

【００２２】なるべくなら、プロセッサ２２、ＲＯＭ２４，ジェネレータ２６及び駆動装置３０はマルチ・チップ・モジユール又は単一ＡＳＩＣとして作成する。１実施例では、プロセッサ２２は、カリフォルニア州サンタ・クララ市インテル社製造の８０５１型マイクロプロセッサのようなオンーチップの１５６バイト・ランダム・アクセス・メモリ付き８ビット・マイクロ・プロセッサである。一定量のランダム・アクセス・メモリ、例えば、１６ＫバイトのＲＡＭは８０５１マイクロプロセッサのオフーチップから離して配置することができる。非揮発性のメモリ素子、例えばＲＯＭ２４は３２Ｋバイトのメモリである。

【００２３】各機密保護装置１４はＰＲＯＭ２４に貯蔵された印加“固定”コードを取り出す。その固定コードはトークンを作成するために使用しアクセスを要求している人を識別するためホスト・システムへ入れることができる。文字の数は実施例により変わるが、デイスプレイ２０は７－１０文字のＬＣＤパネルである。通常のＬＣＤデイスプレイ駆動回路３０はプロセッサ２２とＬＣＤデイスプレイ２０間を連結する。時間変動コード・ジェネレータ２６はマサチュセッツ州ケンブリッジ市セキュアリテイ・ダイナミックス・テクノロジイズ社のタイム・ベイスド・ジェネレータでよく、米国特許第４、７２０、８６０に記載されているので参考のためその全開示事項を本書に記す。

【００２４】ジェネレータ２６は、リヤル・タイム・クロック２５を使用しトークンを誘導するために使用する時間変動コードを生成する。当該時間変動コードは日時に基づくものである。米国特許第４、７２０、８６０号はジェネレータ２６とホスト・システムを相互接続せずに、生体計測機密保護装置１４とホスト・システムが与えられた時間に与えられたインプットに対し同じトークンを作成できるよう、その日時をホスト・システムの時間と同一に保つ方法を説明している。プロセッサ２２は、時間変動コード、固定コード、及び生体計測センサー１８からの生体計測インプットに基づき機密保護トークンを作成し、当該トークンをデイスプレイ２０へ出力する。

【００２５】別の方法では、プロセッサ２２には暗号化計算方式をリヤル・タイム・クロック２５からの日時に適用する標準暗号化・モジュールを含めることができる。その暗号化・モジュールは米国特許第４、８１９、２６７号及び第４、４０５、８２９号に記載されているので、その両特許の全開示事項を参考までに、ここに記載する。当該機密保護トークンは、デイスプレイ２０に出力される。この実施例に於いては、ホスト・システム１０は生体計測機密保護装置１４の暗号化・モジュールが作成する暗号化コードを解読できる暗号解読モジュールを含む。ホスト・システムでの当該トークンの暗号解読能力はユーザーがインプットするトークンを生体計測要素、時間変動要素及び固定コード要素に分解できるものである。

【００２６】応用によっては、これは、インプットしたトークンを貯蔵された数値或いは時間で作成された数値と比較することだけの能力のシステムよりも明らかに優れている。図３は生体計測機密保護装置１４のＩＣカード１４´の実施例を示す。当該ＩＣカード１４´はホスト・システム１０にアクセスしたい人が持つ便利なアクセス可能機密保護装置の役目を果たす。当該ＩＣカードは従来のクレジット・カードの長さ、幅、厚みにすることができる。

【００２７】生体計測センサーの実施例　生体計測センサー１８はユーザー（即ち、カードの所有者、ペンの所有者）からの生体計測インプットを検出する。基本的に個人の情報であって検知する特性が実質的に不変量である情報を感知する範囲では、その正確な特性は、この発明にとって重要ではない。各種の実施例により、当該センサー１８は指紋、署名、声、或いはその他類似の情報を検知できる。ＩＣカードの実施例１４´においては、当該センサー１８は指紋を検出する走査装置であり、或いは署名を検出する圧力感知装置である。

【００２８】別のものとしては、ＣＣＤ（ｃｈａｒｇｅ　ｃｏｕｐｌｅｄ　ｄｅｖｉｃｅ電荷結合素子）イメイジ装置を使用して指紋又は署名のピクチャ（画像）を捕捉できる。当該センサー１８は、又音声検出機でもよ

い。

【００２９】エンロール・モード

機密保護装置１４は先ず“エンロール”（記録）モードの状態にする。エンロール・モードの状態で、１又はそれ以上、好ましくは、数個の生体計測サンプルを取得し雛形として長期の貯蔵とする。別の実施例では、複数のユーザーに対しては複数の雛形を貯蔵する。通常の操作では、生体計測インプット・サンプルを１個又はそれ以上の雛形と比較してサンプルを入れている人が雛形を貯蔵している人であるかどうか識別する。雛形を長期保存するため、またエンロール・モードへのリエントリ（再入）を防ぐため、エンロールのソフトウエアは通常一度使用すると二度とアクセスできない。何度も使うユーザーの実施例については、当該エンロール・モードで有効な生体計測インプットを入れれば、許可されているユーザーだけはリエントリ或いはリセット可能である。もし、そのインプットがエンロール・モードでのリエントリ又はリセットを許可する優先レベルの時は、エンロール・モードに入れる。

【００３０】ノーマル・モード

エンロールが完了すると、当該機密保護装置１４は長期のノーマル・モードに入る。ノーマル・モードでは、ユーザーはスイッチ１６を使用して装置１４の電源を入れて、それから付いている生体計測センサー１８のタイプによる生体計測インプットを入れる。当該生体計測インプットは生体計測センサー１８から受けてインプット部３３へ入れる。指紋、署名又は声のエントリには無関係に、当該生体計測インプットは、一つ又はそれ以上の貯蔵されている雛形と比較する。

【００３１】各雛形に対し相関ファクタを計算する。もし当該相関ファクタが或る雛形に対し事前に決められた、限界レベル（即ち、０－１００の目盛りで９０）よりも接近しているときは、その生体計測の照合は合格である。もし、相関ファクタがいずれも規定のレベルを満足しない時は、当該生体計測の照合は不合格であり、無効の生体計測インプットを示すメッセージが表示される。そのエントリが無効であることをカードの所有者に知らせるのが好ましくない時は、無効のトークンを表示し、またそれはアクセス装置１２に入り、ホスト・システム１０へのアクセスを不可とするが、ホスト・システムは不合格の事実を記録する。

【００３２】前述のように機密保護装置にはそれぞれユニークな所定のコード（例えば、固定コード）がある。当該相関ファクタ、固定コード、及び時間変動コード・ジェネレータ２６からの時間で変わるコードを一緒に使用して機密保護トークンを誘導し表示する。そのユーザーはデイスプレイ２０からトークンを読み、そのトークンをアクセス装置１２に入れる。当該アクセス装置１２はホスト・システム１０にそのトークンを送信して解読し固定コード及び相関ファクタを誘導する。

【００３３】もし当該固定コードが有効ユーザーを識別し、当該相関ファクタが、限界レベル以上であれば、アクセスは許される。もし、そうでなければアクセスは拒否される。固定コードで特定の人或いはグループを識別するため、当該ホスト・システムをプログラム化してアクセスの仕方或いはその固定コードに許されている取引きを制御できる。

【００３４】

【発明の効果】この発明の方法と装置は従来の機密保護システムよりも大巾に利点がある。即ちユーザーがコードを記憶したり、コードの印刷メモを持ち歩く必要のない信頼性のある確実な識別が可能である。また現在使用中のホスト・システムのアクセス装置に便利で確実且つ有用な送信機密保護の機能をつけることもできる。

【００３５】特に、この方法と装置は現在のアクセス装置に特別設計の機器を追加或いは改造をする必要がない。この発明によって作成した機密保護トークンは、普通使用されている個人識別番号或いはその他の機密保護コードと同じ方法でインプット可能である。当該機密保護トークンは離れた場所からアクセス装置へ電子式送信により電話或いはコンピュータでインプットできる。この発明を実施例で図示説明したが、特許請求の範囲で定義される発明の範囲内で各種の変更、修正及び均等なものの使用は可能である。

【図面の簡単な説明】

【図１】この発明の実施例によるトークンを作成する生体計測機密保護装置を含む機密保護システムのブロック線図である。

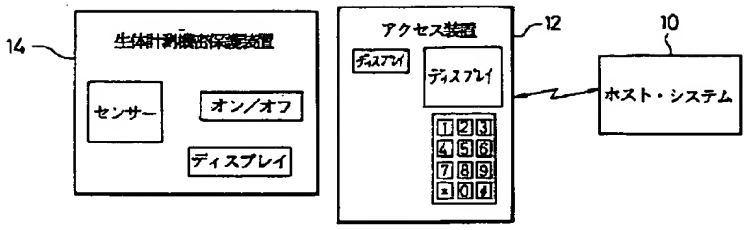
【図２】この発明の当該生体計測機密保護装置の電子式ブロック線図である。

【図３】この発明の図１の生体計測機密保護装置のＩＣカードの実施例である。

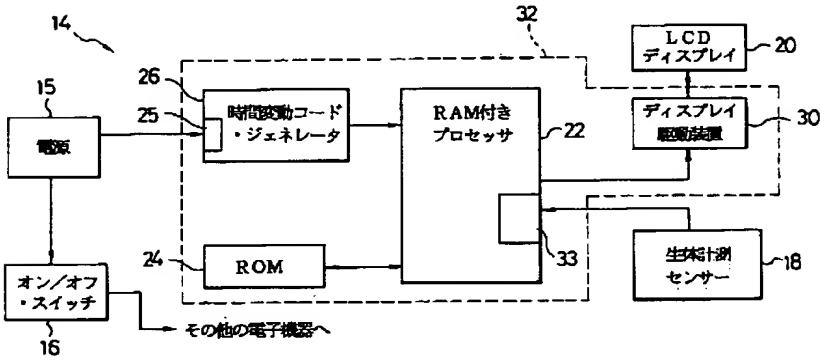
【符号の説明】

１０　ホスト・システム
１２　アクセス装置
１４　生体計測機密保護装置
１４´　ＩＣカード
１５　電源
１６　オン／オフ・スイッチ
１８　生体計測センサー
２０　ＬＣＤデイスプレイ
２２　ＲＡＭ付きプロセッサ
２４　ＲＯＭ
２５　リヤル・タイム・クロック
２６　時間変動コード・ジェネレータ
３０　デイスプレイ駆動装置
３２　マルチ・チップ・モジュール
３３　生体計測インプット部

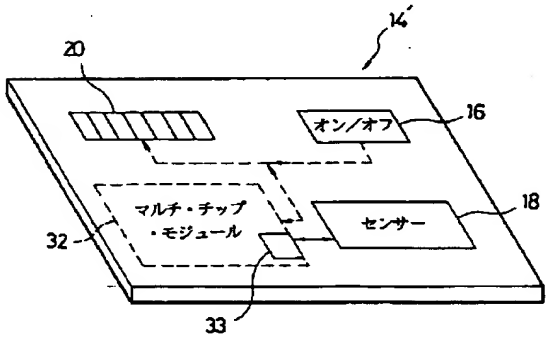
【図１】



【図２】



【図３】



フロントページの続き

(72)発明者　ノーマン　ファスト
アメリカ合衆国、マサチュセッツ州
02168ニュートン、ウエイバン　アベニュ
119